

REMARKS/ARGUMENTS

The Office Action dated May 30, 2008 has been received and carefully studied.

The Examiner objects to the specification as failing to provide proper antecedent basis for the limitation "computer readable medium". By virtue of the accompanying amendment, the Summary has been amended to include a description of the subject matter recited in claims 24 and 25. No new matter has been added.

The Examiner rejects claims 1 and 24 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to point out and distinctly claim the subject matter which applicant regards as the invention. The Examiner notes that the limitation "said established connection" in line 12 of claim 1 lacks sufficient antecedent basis. By virtue of the accompanying amendment, these deficiencies have been corrected.

The Examiner rejects claims 1-3,5-8, and 20-25 under 35 U.S.C. §102(e) as being anticipated by Hennessey et al (U.S. Patent Publication No. 2003/0028623). With respect to claims 1 and 24, the Examiner states that Hennessey teaches a method and a respective computer program for operating a computer network server in a computer network having a central node wherein said network comprises at least one client authorized to access said server via said central node, comprising accessing said central node, obtaining the network addresses of said at least one client, initiating a computer network connection with said at least one client,

receiving a request from said at least one client over the connection and responding to the request.

This rejection is respectfully traversed. Claims 1 and 24 both recite the steps performed by the server. Specifically, the server accesses the central node, receives a list of authorized clients, initiates a connection with those clients, receives a request over that initiated connection from a client and responds to that request. In other words, the client (the device requesting data) never initiates contact with the server. Rather, it accesses the central node, which supplies the client's address to the server, which initiates the connection. In this way, the server can never be directly accessed by clients. Rather, it is the server (or the repository of data) that initiates the connection with the client.

Hennessey discloses a very different process. According to Hennessey, the client accesses the central node to get a list of potential servers, it then accesses one of those servers and requests the desired data from that server. In other words, the central node supplies the client with the address of the server so that the client can initiate the connection. The Examiner notes that the client can also act as a server, as described by Hennessey. While this is true, during the transaction in question, it is acting exclusively as the client.

In comparing the steps recited in the claim, the differences between the present invention and the reference are obvious. The claim requires that the server access the central node to obtain a list of clients. The Examiner

states that Hennessey discloses this action in paragraphs 49 and 59. However, at this point, the device is accessing the central node as the client. While the Examiner is correct that the peer can be a server, it is not acting in that capacity at this time. Hennessey defines client as a node requesting content and a server as a node "that can potentially serve content to other clients". Paragraph 45. Clearly, in paragraph 49, the node is requesting data, and is therefore a client. Furthermore, the node requesting the data (i.e. the client) initiates all activity in the disclosed method of Hennessey. The node requesting data contacts the central node to get addresses of servers. It then establishes connections with those servers and requests the data, which is then sent to it by the server.

As noted above, in the present invention, the client does not initiate the connection to the server, as the server does not have a listening port. Thus, the method outlined in Hennessey does not anticipate claims 1 and 24.

The Examiner rejects claims 3 and 25 stating that Hennessey teaches a method and computer program product to operate a computer server in a computer network having a central node wherein the server has a listening port. The method includes the steps of maintaining a connection with a central node, receiving a command from said central node to open a listening port after central node receives a request from a client to access said server, opening a listening port, sending to the central node instructions for the client to connect to the server over the listening port and receiving communication from the client after the

central node delivers a command to the client to connect to the server.

This rejection is respectfully traversed. The present invention describes a mechanism wherein a client can connect to a server, during a very short period of time. To do so, the client sends a request to the central server. The central server then instructs the server to open a listening port. After the server opens this listening port, it then informs the central node that the client may connect over this port. The central node informs the client that it can connect and the network connection is established. Thus, the chances of a troll or DOS attack occurring are minimal as the listening port on the server is only open a very short time.

Hennessey does not disclose such a mechanism. In fact, Hennessey does not disclose that the central node instructs the server to open a listening port. The Examiner cites paragraphs 52, 77, and 78 for support. However, the only mention of ports in these paragraphs is the port in the firewall 302. This is not the same as the listening port on the server itself. Rather, UDP is used to open ports in the firewalls between the server and the client and is not related to the listening ports on the server. Furthermore, since Hennessey does not teach that the server is instructed to open a listening port, there cannot be disclosure that the server, having opened this port, then communicates back to the central node instructions for the client to connect via that port.

As stated above, Hennessey teaches a mechanism which is client driven. In other words, the client accesses the directory server to get a list of candidate servers. The client then accesses one or more of these servers. That mechanism does not overcome the problems that the present claims address; namely the vulnerability of that server to attack, since it is readily accessible by external nodes. The present invention addresses this issue in a number of ways, including the methods recited in claims 1 and 3. In contrast, Hennessey discloses a mechanism by which a client that requests data is able to find out the closest servers having the desired data. There is no mention of the issues associated with server attacks. Finally, there is no disclosure that the server initiates the connection to the client, nor is there disclosure that the server temporarily opens a listening port in response to an instruction from the central node.

The Examiner rejects claim 20, stating it is an apparatus claim that corresponds to the method recited in claim 3. For the reasons explained above regarding claim 3, this claim is believed to be allowable.

The remaining claims are all believed to be in condition for allowance by virtue of their dependence of the independent claims, which have been discussed above.

Reconsideration and allowance are requested in view of the foregoing arguments.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Robert Frame', written over a circular stamp or seal.

Robert Frame

Reg. No. 54,104

176 E. Main Street-Suite 5

Westboro, Massachusetts 01581

TEL: (508) 898-1818